**测试结果**

**第1关：基本测试**

根据S-DES算法编写和调试程序，提供GUI解密支持用户交互。输入可以是8bit的数据和10bit的密钥，输出是8bit的密文。

说明：在输入框内写入8bit数据，选择“二进制”单选按钮后输入任意10bit密钥，选中“加密”或“解密”单选框后，点击“立即执行”便得到相应结果。



图1 加密二进制交互图示

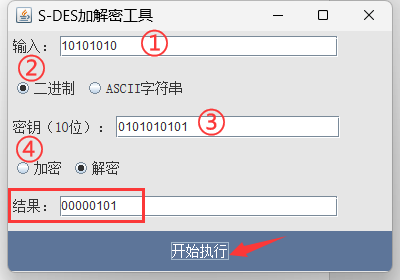


图2 解密二进制交互图示

**第2关：交叉测试**

考虑到是算法标准，所有人在编写程序的时候需要使用相同算法流程和转换单元(P-Box、S-Box等)，以保证算法和程序在异构的系统或平台上都可以正常运行。设有A和B两组位同学(选择相同的密钥K)；则A、B组同学编写的程序对明文P进行加密得到相同的密文C；或者B组同学接收到A组程序加密的密文C，使用B组程序进行解密可得到与A相同的P。

说明：以下是A组同学的实验数据，我们使用“1010101010”作为相同密钥，对该密文进行解密操作，得到输出与A组明文一致，验证成功。



图1 A组同学实验结果

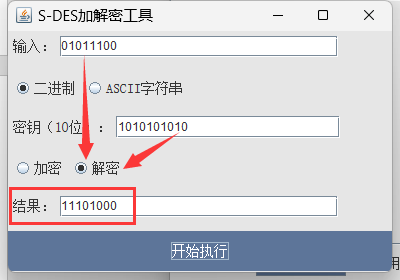


图2 解密A组密文输出明文结果

**第3关：扩展功能**

考虑到向实用性扩展，加密算法的数据输入可以是ASII编码字符串(分组为1 Byte)，对应地输出也可以是ACII字符串(很可能是乱码)。

说明：在输入框内写入ASII编码字符串，选择“ASII字符串”单选按钮后输入任意10bit密钥，选中“加密”或“解密”单选框后，点击“立即执行”便得到相应结果。

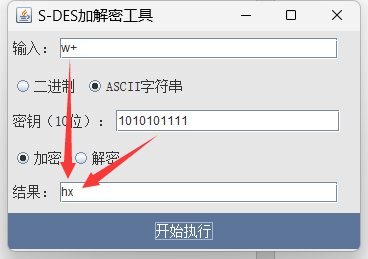


图1 加密字符串交互图示

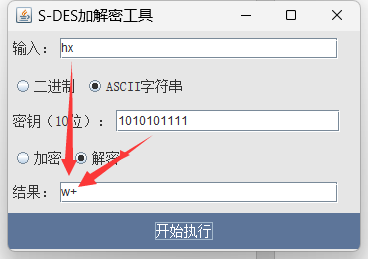


图2 解密字符串交互图示

**第4关：暴力破解**

假设你找到了使用相同密钥的明、密文对(一个或多个)，请尝试使用暴力破解的方法找到正确的密钥Key。在编写程序时，你也可以考虑使用多线程的方式提升破解的效率。请设定时间戳，用视频或动图展示你在多长时间内完成了暴力破解。

说明：选择复选框（使用相同密钥的明、密文对数目），填入对应明密文对，点击“查找密钥”，得到暴力破解时长和相应密钥。



图1 交互图示

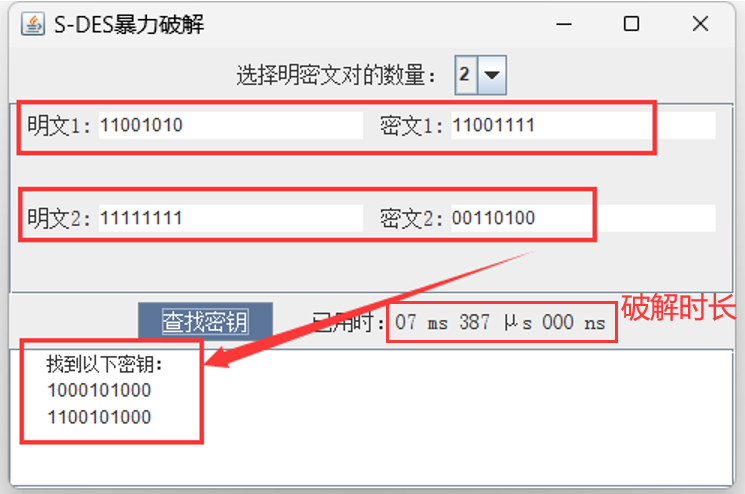


图2 破解两对明密文所得密钥及时长

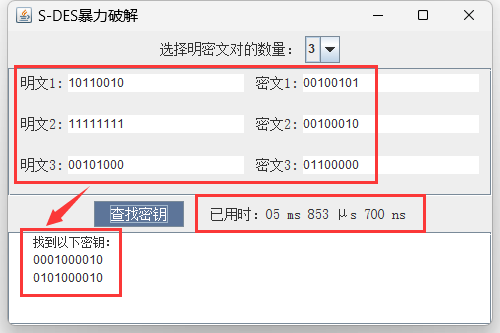


图3 破解三对明密文所得密钥及时长

**第5关：封闭测试**

根据第4关的结果，进一步分析，对于你随机选择的一个明密文对，是不是有不止一个密钥Key？进一步扩展，对应明文空间任意给定的明文分组Pn，是否会出现选择不同的密钥Ki≠ Kj加密得到相同密文Cn的情况？

说明：对于随机选择的一个明密文对（明文：00100101；密文：10110000），可以找到不止一个密钥K。

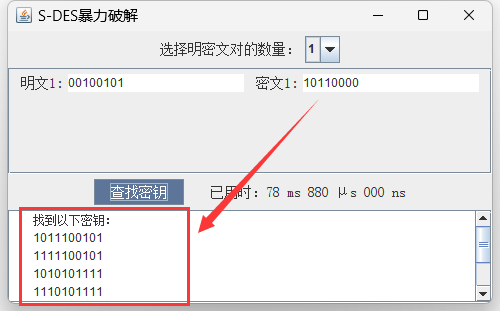


图1 破解一对明密文所得密钥

说明：对于明文空间任意给定的明文分组P1,P2,P3（如图为明文1，2，3），出现了选择不同的密钥K1, K2（如图为密钥0001000010，0101000010）加密得到相同密文C1,C2,C3（如图分别对应密文1，2，3）的情况.

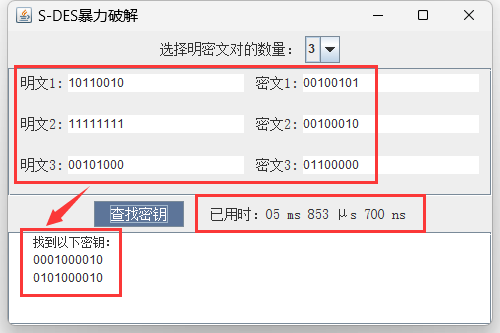


图2 破解三对明密文所得密钥

结论：实验观察发现，密钥的第2位（从高位起）对明文的加密结果无影响。



图3 破解三对明密文对所得密钥仅第二位不同



图4 破解四对明密文对所得密钥仅第二位不同